ASSURANCE CONTINUITY MAINTENANCE REPORT FOR

Galleon Embedded Computing XSR and G1 Software Encryption Layer

Maintenance Report Number: CCEVS-VR-VID11273-2024

Date of Activity: 11 July 2024

References:

Common Criteria Evaluation and Validation Scheme Publication #6, Assurance Continuity: Guidance for Maintenance and Re-evaluation, version 3.0, 12 September 2016

Common Criteria document 2012-06-01 "Assurance Continuity: CCRA Requirements" Version 2.1, June 2012

collaborative Protection Profile for Full Drive Encryption - Encryption Engine, Version 2.0 + Errata 20190201, February 1, 2019 [FDEEEcPP20E]

collaborative Protection Profile for Full Drive Encryption - Authorization Acquisition, Version 2.0 + Errata 20190201, February 1, 2019 [FDEAAcPP20E]

Impact Analysis Report for Galleon Embedded Computing XSR and G1 Software Encryption Layer, Version 1.1, July 18, 2024

Galleon Embedded Computing XSR and G1 Software Encryption Layer Security Target, Version 1.5, July 14, 2022

Galleon Encryption Module v4 Release Notes, June 25, 2024

Assurance Continuity Maintenance Report:

Gossamer Security Solutions submitted an Impact Analysis Report (IAR) and Assurance Continuity Maintenance package for the Galleon Embedded Computing XSR and G1 Software Encryption Layer to the CCEVS for approval in June 2024. The IAR is intended to satisfy the requirements outlined in Common Criteria Evaluation and Validation Scheme Publication #6, Assurance Continuity: Guidance for Maintenance and Re-evaluation, version 3.0. In accordance with those requirements, the IAR describes the changes made to the certified TOE, the evidence updated because of the changes, and the security impact of the changes.

The evaluation evidence submitted for consideration consists of the Security Target (ST) and the Impact Analysis Report (IAR). No updates to the ST were required.

Documentation Updated:

Original CC Evaluation Evidence	Evidence Change Summary
Galleon Embedded Computing XSR and G1 Software Encryption Layer Security Target, Version 1.5, July 14, 2022	No changes required.
Design Documentation: See Security Target and Guidance	No changes required
Guidance Documentation: Galleon SW Encryption Layer Certifiable Encryption, Version 1.0.7, July 14, 2022	No changes required
Lifecycle: None	No changes required.
Testing: None	Galleon performed two levels of regression testing. See Regression Testing below.
Vulnerability Assessment: None	The public search was performed on 18 July 2024. No public vulnerabilities exist within the product. See analysis of results below.

Changes to the TOE:
Galleon Embedded Computing made updates to the Galleon Embedded Computing XSR and G1 Software Encryption Layer to apply RHEL8.4 patches. These patches were necessary due to updates/upgrades to the underlying Encryption Module, which is not within the TOE boundary.

Major Changes

None.

Minor Changes

Change Description	Security Analysis
Integrated Red Hat patches to update RHEL 8.4 to ensure OpenSSL was patched for CVEs.	This upgrade was done to address CVEs as required by NIAP. No algorithm implementations have changed. The patches do not impact SFRs; as such, re-evaluation is not required.
Integrated Red Hat patches to update RHEL 8.4 to ensure libgcrypt was patched for CVEs.	This upgrade was done to address CVEs as required by NIAP. The patches do not impact SFRs; as such, re-evaluation is not required.

Integrated Red Hat patches to update RHEL 8.4 for all security issues published.	This upgrade was done to address CVEs as required by NIAP. The patches do not impact SFRs; as such, re-evaluation is not required.

Regression Testing:
Galleon performs two levels of regression testing. Each encryption layer (in this case software) is tested independently during development. After successful single layer testing, the product is tested using “user stories" that cover expected functionality from the user's point of view and covers system integration issues.

Equivalency:

The security functionality of the current Galleon Embedded Computing XSR and G1 Software Encryption Layer update remains the same as the prior evaluated version. The models and processors are unchanged from the original evaluation version.

NIST CAVP Certificates:

The same cryptographic modules are used in the current Galleon Embedded Computing XSR and G1 Software Encryption Layer update. The CAVP certificate numbers referenced during the Galleon Embedded Computing XSR and G1 Software Encryption Layer evaluation have not changed.

Vulnerability Analysis

A search for known publicly disclosed vulnerabilities was performed against the National Vulnerability Database and the Vulnerability Notes Database on July 18, 2024. The search terms used were:

- disk encryption
- drive encryption
- key destruction
- key sanitization
- Password caching
- Key caching
- Galleon
- G1
- XSR
- Intel Atom CPU C2758
- Intel Xeon CPU E3-1505L v6
- Opal management software
- SED management software
- LUKS
- Linux Unified Key Setup
- kernel cryptography
- openssl
- libgcrypt
- RHEL 8.4
- Intel Xeon E3-1505Mv6
- Intel Xeon E-2276ME
- Intel Xeon E-2276ML

Of the results found for the search terms, none were identified as applicable to the changed TOE or were fixed by the patches applied as described in the change descriptions above. There are no publicly disclosed cybersecurity vulnerabilities applicable (in use) to the changed TOE. Therefore, no additional mitigation is required to the changed TOE.

Conclusion:

CCEVS reviewed the description of the changes and the analysis of the impact upon security and found the changes to be minor and did not affect the evaluated security functionality. Therefore, CCEVS agrees that the original assurance is maintained for the above-cited version of the product.